30 卫士安全产品系列之

30 卫士存储介质信息消除工具

（平板电脑版）

使用手册

中国电子科技集团公司第三十研究所

目　　录

第一章　产品介绍 1

产品概述 1

产品主要功能 1

产品外观图 4

产品配件 4

第二章　简明使用流程 5

第三章　平板电脑使用简介 6

平板电脑的外观 6

状态指示灯 7

使用触摸笔 7

第四章　信息消除工具 9

配置计算机从 USB 设备启动 9

如何启动消除工具 11

认识消除工具主界面 14

信息消除操作 17

多个磁盘并行擦除 18

多个分区串行擦除 19

日志审计 19

日志查询 21

报表输出 22

第五章　计算机终端深度检查取证工具 23

配置计算机从 USB 设备启动 23
如何启动取证工具 23
认识取证工具主界面 23
计算机基本信息检查 28
计算机上网信息检查 30
文件操作信息检查 34
移动介质信息检查 37
计算机综合检查 38
计算机其它信息取证 40
第六章　恶意程序攻击行为检测 45
配置计算机从 USB 设备启动 45
如何启动攻击行为检测工具 45
认识行为检测工具主界面 45
第七章　常见问题..... 51
第七章　注意事项..... 52
第八章　联系我们..... 53

第一章　产品介绍

产品概述

目前，移动存储介质、计算机及其网络已成为泄密的重要渠道，是保密管理的重中之重。为了配合《中华人民共和国保守国家秘密法》和《涉及国家秘密的信息系统分级保护技术要求》等保密法规的实施、方便保密机构对涉密单位保密工作的监督和检查以及保密单位内部的保密自查，我所推出了一系列保密安全产品。

其中，30 卫士存储介质信息消除工具是一款多功能应用工具，以安全平板电脑为硬件平台，集成了存储介质信息消除工具、计算机终端深度检查取证工具和恶意程序攻击行为检测工具为一体的 3 合 1 工具平台，具有强大完善的功能、简单友好的界面、全面优质的技术支持，满足保密管理工作需要。

产品主要功能

存储介质信息消除工具

- 具有 1 次、3 次、6 次和 7 次的擦除方案选择；

1 **1 次擦除** 为安全强度较低的数据擦除，但其擦除速度最快，适用于对安全性要求不高但对擦除速度有较高要求的场合。

2 **3 次擦除** 依据美军 DOD-5200.22 标准，适用于对擦除速度及擦除效果有要求的场合。

3 **6 次擦除** 依据国家保密局标准擦除算法，适用于对擦除效果有较高要求的场合。

4 **7 次擦除** 安全强度最高的数据擦除方案，安全擦除序列是针对不同磁盘编码规则设计的，适用于对擦除效果有高要求的场合。

- 支持全盘擦除与分区擦除两种方案；
- 基于独立操作系统架构，利用“0 磁道”全覆盖物理擦除方案，高强

度处理每一个存储单元；

- 强大的数据擦除能力；

对上网产生的各种浏览记录、下载记录、邮件收发记录，对移动介质或者其它外接设备的使用记录，对日志信息、文件信息、文件管理信息、数据信息，对病毒控制区、逻辑坏道区等系统不可见区域的信息进行彻底擦除、不留死角。

- 支持擦除行为记录和审计能力；
- 提供审计信息的报表输出能力；

计算机终端深度检查取证功能

- 上网记录的检查

检查计算机存在的违规上网记录信息，包括历史上网信息、Cookies 文件夹下遗留的上网文件信息、临时文件夹下的上网记录信息、收藏夹下的网络信息及浏览器下拉列表的网络信息；检查系统内安装的传输工具，包括蓝牙设备、常用网络工具；检查系统与外部网络互联信息、检查系统内网络设备信息；能够对直接删除、格式化、重装系统后的上网记录进行检查。

- 文件记录的检查

检查文件操作记录信息，包括历史文件操作记录、最近操作的文件信息及系统库中的文档操作记录信息；搜索特定关键字的文件，通过文件信息检索技术，对包含有“秘密”、“机密”、“绝密”等特定敏感关键字的文件进行搜索，支持对指定的分区搜索，支持对 Office 2007、Office 2003、TXT、WPS、CEB 等格式的文件搜索；支持文件信息深度检索，利用数据恢复技术，能对直接删除、格式化、重装系统后的文件信息进行搜索。

- 移动存储设备的检查

检查移动存储介质及其它外接设备的使用记录，并在取证报告中显示移动介质的设备名称、序列号、使用时间等详细信息。

- 系统安全性检查

检测操作系统升级情况、存在的漏洞；分析系统运行进程，并对可疑进程进行详细分析；检查系统是否存在非法用户，检查用户口令的长度和强度是否符合保密要求；检查系统的共享文件目录。

- 收集存储检查取证记录

能够收集并存储检查取证结果，并提供日志审计、报表查询功能。

- 自动生成检查报告

检查完成后，能够自动生成检查报告，并支持打印输出。

恶意程序攻击行为检测功能

- 计算机综合检查

检查系统进程、、开放端口信息、系统共享信息、远程连接、默认磁盘共享、默认用户共享、注册表关键位置、关键服务及杀毒软件信息。

- 可疑程序扫描

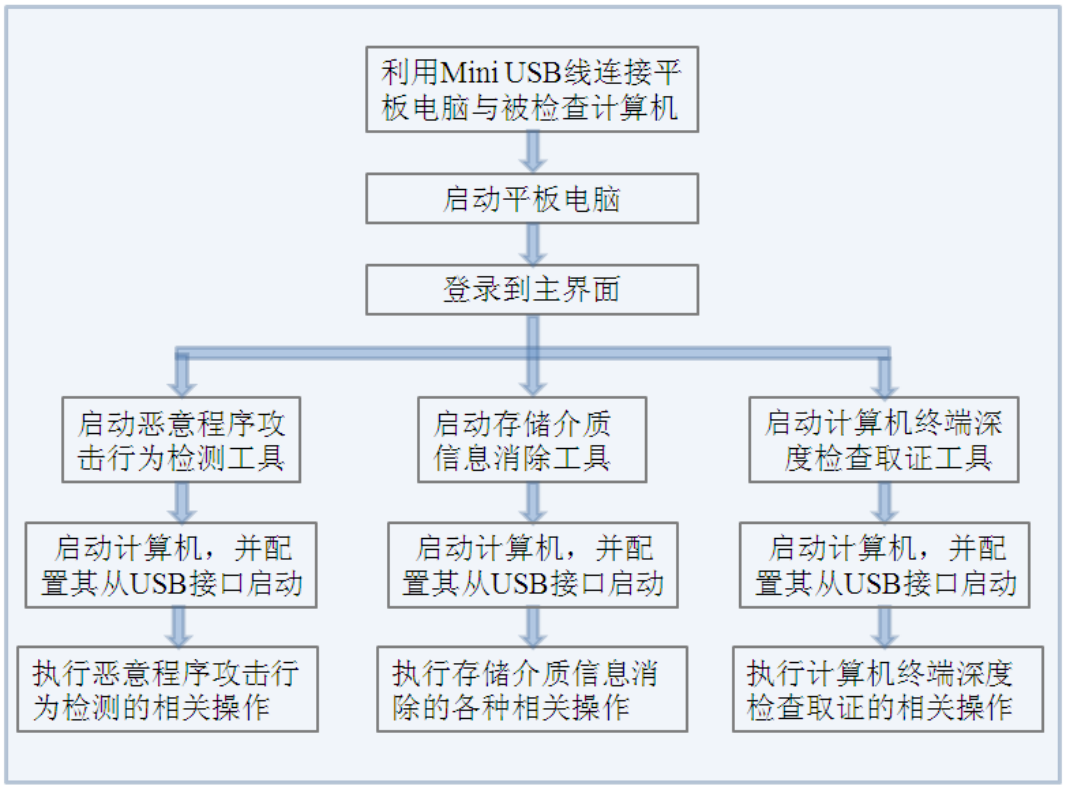
对被检查计算机系统内存在可疑程序进行检测，可检查木马、病毒和可疑的恶意程序的位置，并生成检测报告。

产品外观图

产品配件

序号	名称	数量
1.	平板电脑	1 台
2.	电源适配器	1 个
3.	Mini USB 线	1 根
4.	Mini VGA 线	1 根

第二章　简明使用流程


利用Mini USB线连接平板电脑与被检查计算机
启动平板电脑
登录到主界面
启动恶意程序攻击行为检测工具
启动存储介质信息消除工具
启动计算机终端深度检查取证工具
启动计算机，并配置其从USB接口启动
启动计算机，并配置其从USB接口启动
启动计算机，并配置其从USB接口启动
执行恶意程序攻击行为检测的相关操作
执行存储介质信息消除的各种相关操作
执行计算机终端深度检查取证的相关操作

第三章　平板电脑使用简介

本章内容将帮助您循序渐进地学习使用您的平板电脑。

平板电脑的外观

正视图

1 **指纹识别模块** 为用户提供计算机安全，快捷的功能。

2 **信号指示灯** 指示键盘、设备状态。

左视图

1 **Mini 串口**

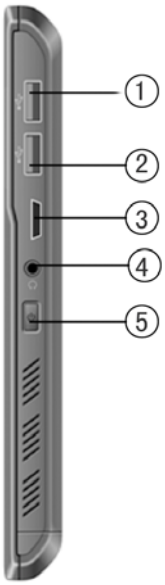
2 **Mini USB 接口**

3 **TF 卡接口** TransFlash 卡接口，可以用来储存个人数据。

4 **电源接口** 连接电源

5 **系统恢复键**

右视图



1 **USB 接口** 用于连接使用 USB 接口的外部设备，支持高速的 USB2.0

2 **MiniVGA 接口** 连接至显示设备

3 **音频接口** 立体声输出和麦克风输入设备，建议使用手机制式耳机

4 **电源按键** 按电源按钮可以打开或关闭产品

状态指示灯

序号	名称	描述
1.	电源状态灯	只有电池红色灯亮；只有适配器红色灯亮
2.	充电/电池状态灯	电池电量低时为紫色闪烁；电池充电过程中蓝色灯亮，电池充满红色灯亮
3.	硬盘状态灯	

使用触摸笔

按键定义

1.末端按键为鼠标右键，用笔点触屏幕同时按动此键；

2.靠近笔尖一端按键为鼠标中键，用笔点触屏幕同时按动此键；

3.笔尖点触屏幕为正常鼠标左键。

开启

按住末端按键。

触控笔的基本操作

将触摸笔尖轻置于本电脑的触摸屏显示板上，并向希望指针移动的方向移动笔尖。

选定（点击）

点击按钮，快速点击并释放触摸笔尖。可以通过点击选定菜单选项和屏幕上的图标，或在文档中定位指针。

双击（运行）

双击触摸笔尖，即快速连续两次轻击触摸显示板。选择并双击可执行文件或程序文件图标启动程序运行。

拖动与停止

使触摸笔尖触摸当前图标并保持（不释放），同时在触摸板上滑动，可以拖动目标移动。直到目标被拖动到想要的位置，释放触摸笔尖。可以使用拖动、停止来把文件从一个位置移动到另外一个位置。

例如：若要将某个文件置于回收站，使用触摸笔尖触摸选中想要移动的文件并保持（不释放），滑动此文件，直至被拖到回收站（图标）上，然后释放触摸笔尖。

拖动：在不释放触摸笔尖同时移动图标。

停止：图标位于回收站上方时，释放触摸笔尖。

右键菜单

使触摸笔尖触摸当前图标并保持(不释放)，此时采用两种方式进入右键菜单。

1.按着不放约 3 秒钟，当前显示为圆圈运行，然后进入右键菜单；

2.按着不放同时用您的一个手指在当前图标的空白处点击一下触摸屏幕，则同样进入右键菜单。

第四章　信息消除工具

本章内容将帮助您循序渐进地学习使用 30 卫士存储介质信息消除工具（以下简称“消除工具”）。

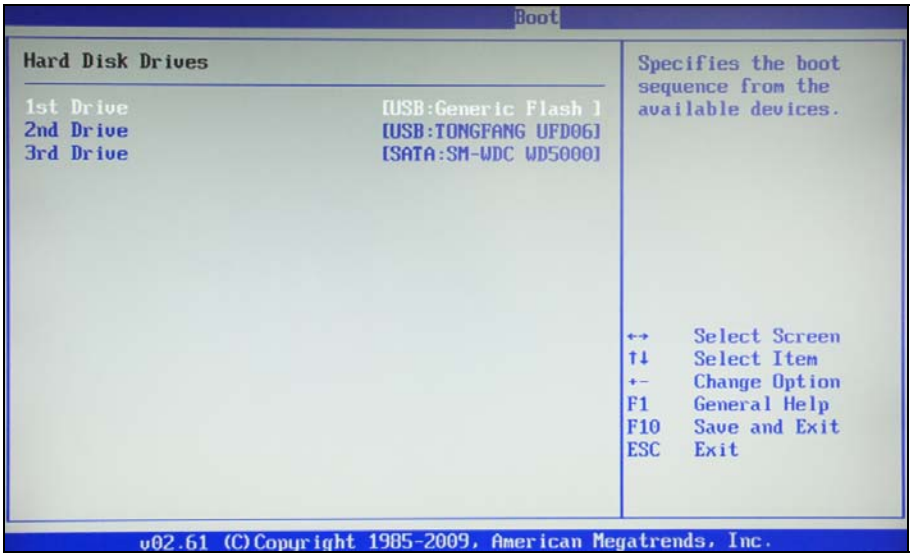
配置计算机从 USB 设备启动

计算机通常有两种方法配置为 USB 设备启动：1）在 BIOS Setup 中设置首选启动项为 USB 设备；2）在 Boot Menu 中选择启动项为 USB 设备。

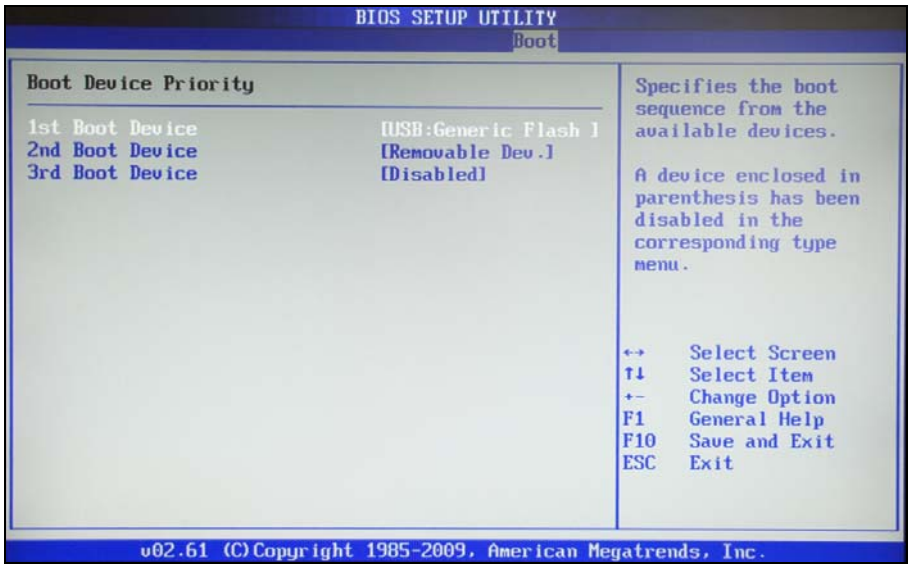
BIOS 中设置首选启动项

启动计算机，并按住“Del”键（或者“F2”键）不放，直到出现 BIOS 设置窗口，根据计算机主板的不同，设置方法也会不同，下面列出两种设置方法以供参照。

示例一：1）在 Boot Setting 中设置硬盘的次序，设置 USB:Generic Flash Disk 为第一硬盘。

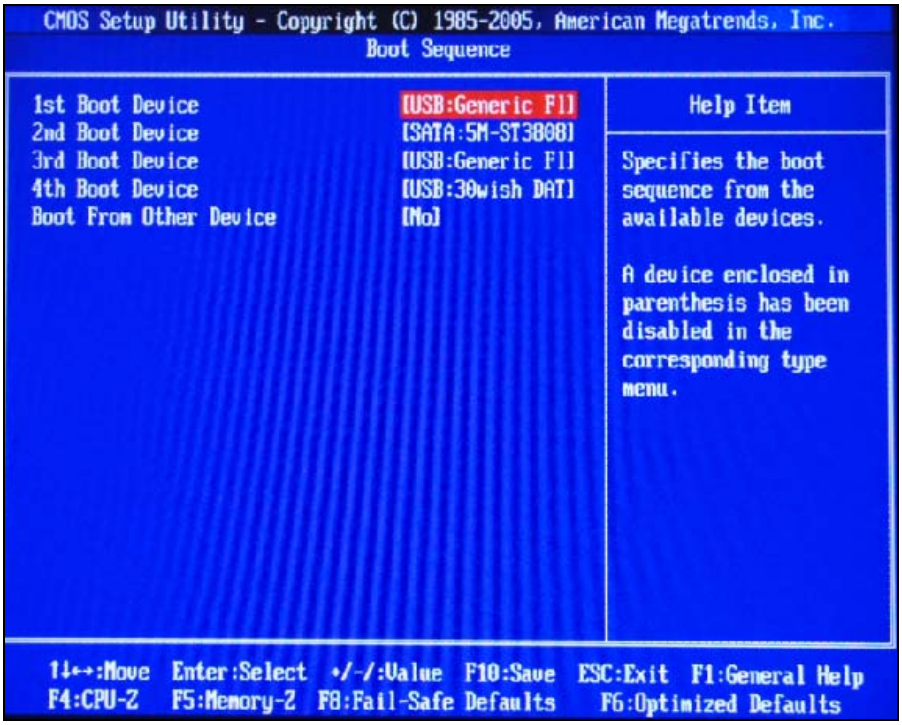


2）在 Boot Setting 中设置启动设备优先级，选择 USB: Generic Flash Disk 为第一启动设备。



3）设置完毕，按下“F10”键保存配置并退出。

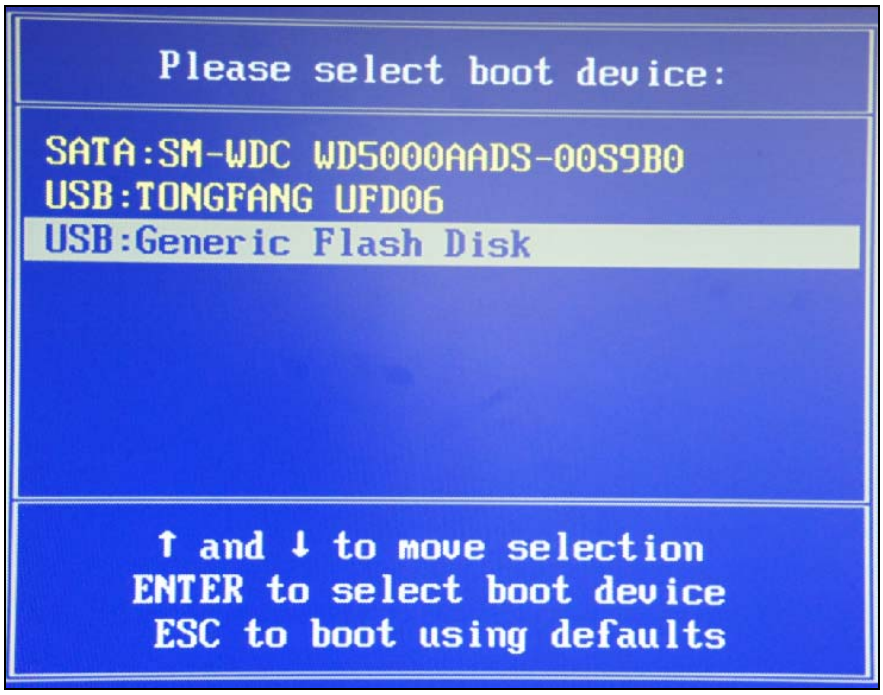
示例二：1）在 BIOS Setup 的启动顺序设置界面中直接设置第一启动设备为 USB: Generic Flash Disk。



2）设置完毕，按下“F10”键保存配置并退出，系统将自动重启并从 USB 设备启动。

Boot Menu 中选择启动项

启动计算机，按下“F8”键（或者“F11”键、“F12”键）进入 Boot Menu 启动选择界面。选择 “USB Generic Flash Disk”作为启动设备，系统将自动从 USB 设备启动。



注意：不同的计算机设置首选启动设备的方式可能不同，具体请参考计算机主板使用说明。且使用完信息消除工具后，请恢复 BIOS 设置。

如何启动消除工具

1） 将 Mini USB 线的小头插座连接到平板左侧的 Mini USB 口，大头插座连接到计算机的任意 USB 口；

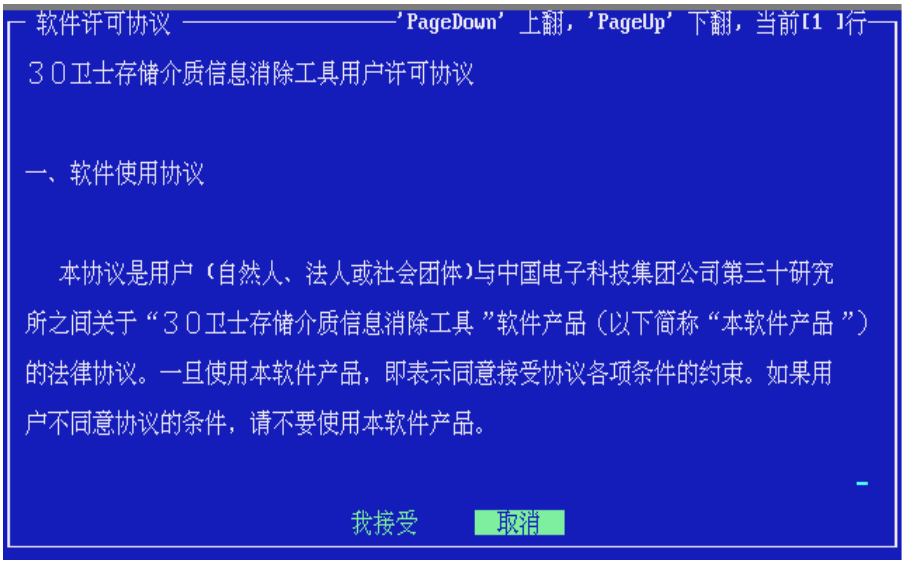
2） 启动平板电脑，等待启动完成并出现主界面；

3） 点击“30 卫士存储介质信息消除”图标，进入工具界面；

4） 启动要进行信息消除的计算机，并配置计算机从 USB 设备（平板电

脑）启动。在启动过程中请耐心等待，计算机出现初始启动界面；

5） 在启动过程中，出现用户许可协议，请认真阅读，确定使用本工具请选择“我接受”，否则选择“取消”退出使用。



6） 启动完成后，平板电脑与计算机的界面将进行同步，主要功能信息区的内容显示完全一致。

认识消除工具主界面

1 功能栏

2 主机信息列表

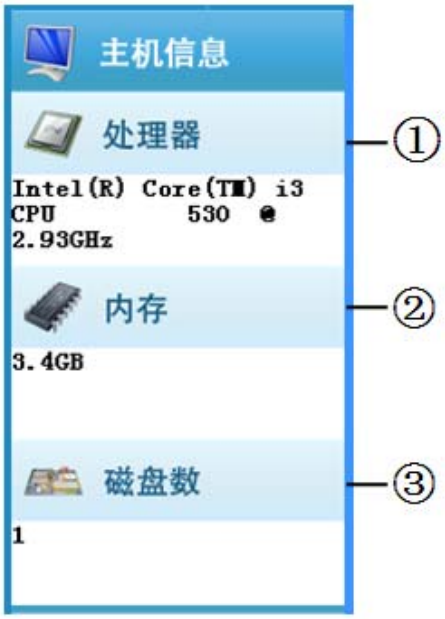
3 磁盘（分区）列表

4 擦除选择区

功能栏

功能栏具有“信息消除”、“日志查询”、“日志审计”、“输出报表”、“设备信息”及“关于”等功能按键。

主机信息列表



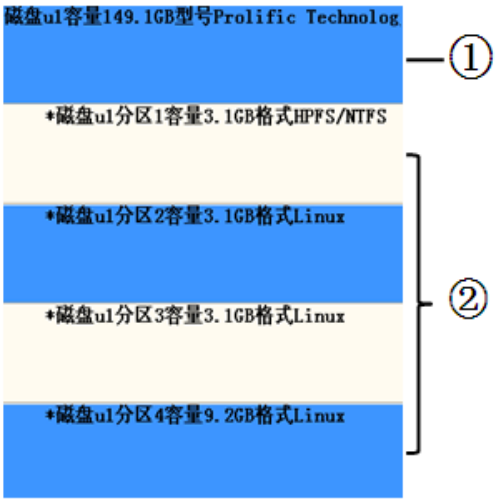
1 **处理器** 显示 CPU 信息

2 **内存** 显示内存容量

3 **磁盘数** 显示当前主机的磁盘数量

磁盘（分区）列表

磁盘（分区）列表会根据磁盘的实际个数自动进行更新，列表会随着磁盘个数以及磁盘上分区数的改变而更新。当列表项在一页内无法完全显示时就会自动进行分页，一页最多可以显示 6 个列表项。



1 **磁盘信息栏** 显示磁盘号、容量、序号信息

2 **磁盘分区信息栏** 显示磁盘分区号、容量、分区格式

- 磁盘号

磁盘号格式一般是一个字母后跟数字，例如 s1、h1、u1。字母代表了不同的磁盘接口类：S – SCSI、SATA 设备，H – IDE 设备，U – U 盘设备。字母

之后的数字是同类总线下磁盘的编号，该编号一般情况下是按顺序排列的，例如：h1 指的主 IDE、h2 指的从 IDE。

- 磁盘容量

磁盘容量信息显示了磁盘的大致容量（容量单位缺省为 BYTE），这个数值是按实际磁盘容量的单位进行调整的。如果容量>=1000GB 则以 T 为单位，容量<1000GB 就以 G 为单位，容量<1000MB 以 M 为单位，容量<1000KB 就以 K 为单位。

- 磁盘序号

磁盘序号由磁盘厂商提供的 Model 及 Serial 信息生成，它是可以区分磁盘的唯一编号。

Model 号：磁盘厂商的特殊信息；

Serial 号：磁盘出厂时的唯一编号。

- 磁盘分区号

磁盘分区号由磁盘号加上分区编号组成。如：磁盘 S1 分区 1。

- 分区格式

该内容显示的是分区格式类型信息，常见的有：Windows 分区如（FAT、FAT16、FAT32、NTFS）、Linux 分区如（Ext、Ext2、Ext3）等。

擦除选择区

1 **1 次擦除** 为安全强度较低的数据擦除，但其擦除速度最快，适用于对安全性要求不高但对擦除速度有较高要求的场合。

2 **3 次擦除** 依据美军 DOD-5200.22 标准，适用于对擦除速度及擦除效果有要求的场合。

3 **6 次擦除** 依据国家保密局标准擦除算法，适用于对擦除效果有较高要求的场合。

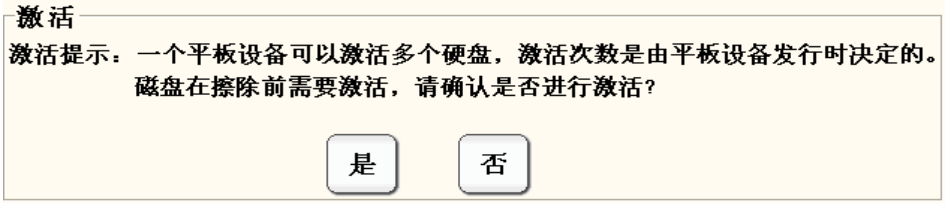
4 **7 次擦除** 安全强度最高的数据擦除方案，安全擦除序列是针对不同磁盘编码规

信息消除操作

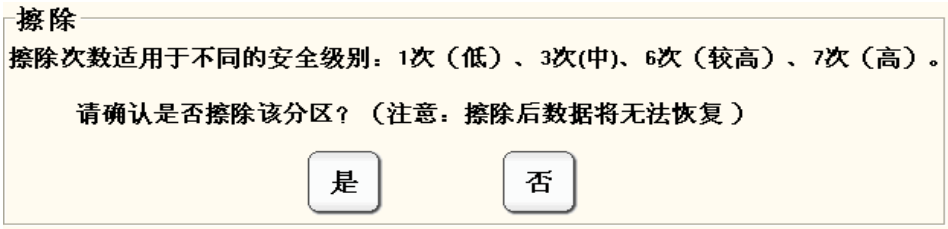
1） 选择擦除对象，如果选中磁盘列表项，那么即对该磁盘进行整盘操作，如果选中的是分区列表项，那么只是对该分区进行操作。

2） 选择擦除强度，回车；

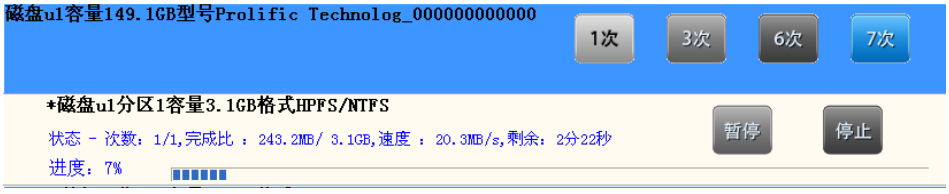
3） 激活该磁盘，本工具在使用之前，将弹出激活窗口提示用户激活磁盘（如果该磁盘已激活过则不会弹出）。注意：如果选择激活，你的平板设备剩余激活次数将会减少一次，该磁盘被激活便可以反复擦除使用，如果你选择的是分区擦除那么激活分区所对应的磁盘。



4） 完成激活后，弹出擦除确认对话框以确认本次擦除操作是否继续进行，选择‘是’或‘否’确认。



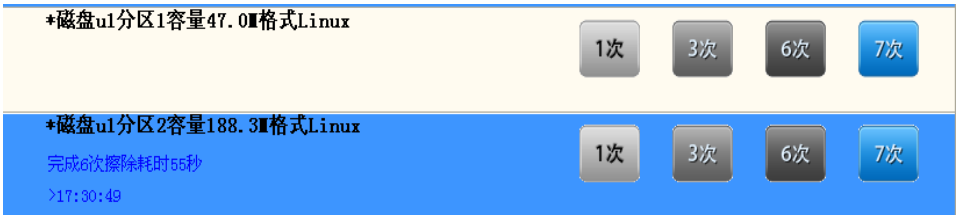
5） 擦除开始后，磁盘（分区）信息栏将显示擦除次数、完成比、速度、剩余时间及进度条等相关信息。



任务擦除状态及擦除进度信息具体内容如下：

- 次数：显示已经擦除的次数及任务的总次数；
- 完成比：显示本次擦除的已完成容量以及总容量；
- 速度：显示的平均擦除速度；
- 剩余：完成本次任务还需要的时间（注意：该数值是根据历史擦除速度估算得来的，仅供参考）；
- 暂停：在任务进行过程中按下‘暂停’按钮，会将磁盘或分区的擦除任务暂停下来。这时按钮由‘暂停’变为了‘继续’；
- 继续：当前擦除状态处于暂停状态时可以按下‘继续’按钮，恢复被暂停的擦除任务继续进行擦除；
- 停止：在任务进行过程中可以对擦除任务进行停止操作。停止会终止本次擦除任务。在界面上由擦除状态变为未擦除状态，按钮区上的按钮又恢复擦除之前的状态：‘1 次’、‘3 次’、‘6 次’、‘7 次’；
- 擦除进度：显示擦除的完成比及擦除进度条标尺。

6） 任务完成后，进度栏上显示完成擦除的时间、完成次数和耗时。



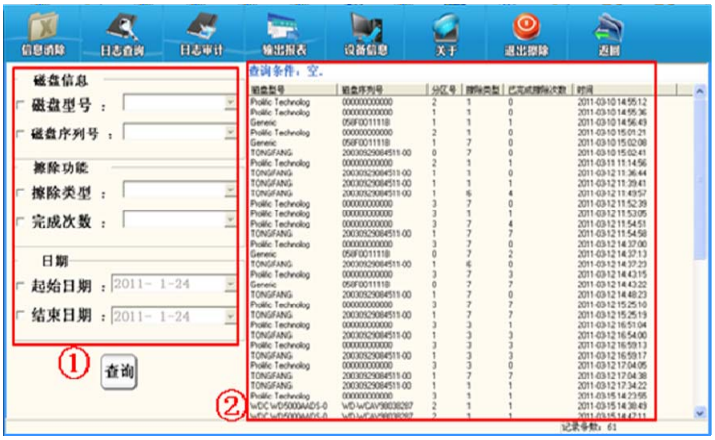
多个磁盘并行擦除

本软件支持多个磁盘同时进行擦除的能力，在不同硬盘上的任务是并行的。

多个分区串行擦除

对于同一个磁盘上的不同分区，在同一时间内只能执行其中一个分区的擦除，为了满足多个分区擦除的需求，我们设计了任务排队的机制。同一磁盘不同分区上开启擦除任务后，软件将按照任务开启的先后顺序依次进行擦除，保证所有分区都能被擦除。

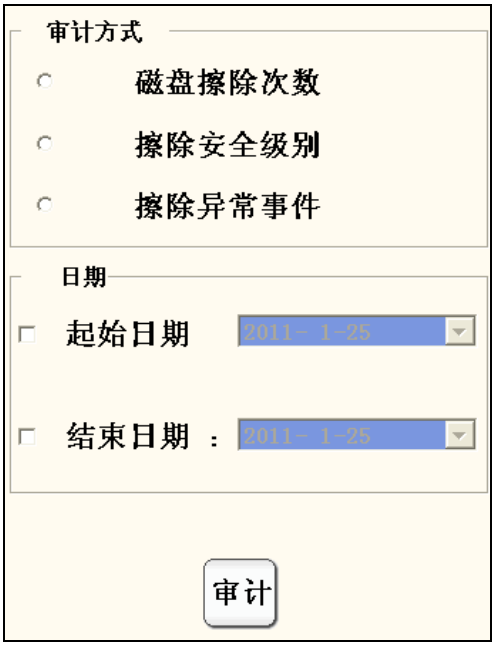
日志审计



1 日志审计条件

2 日志审计结果

日志审计条件



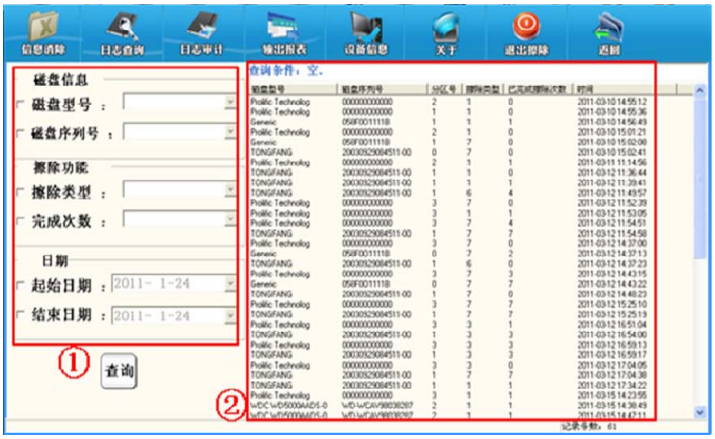
审计方式包括：磁盘擦除次数、擦除安全级别、擦除异常事件，然后可以选择起始与结束日期

日志审计结果

如果列表内容较多，可以通过拖动滚动条进行滚屏显示。移动鼠标到列表头的列与列之间分割线，可以调整列表头的宽度。

审计条件：磁盘擦除次数,时间段：开始使用日期至今
磁盘型号 磁盘序列号 总... 整盘... 分区... 1次擦... 3次擦... 6次擦... 7次擦除
CETC-30 S sw_yzyj_10_188 4 4 0 4 0 0 0
CETC-30 S sw_yzyj_10_488 2 2 0 2 0 0 0
CETC-30 S sw_yzyj_10_588 1 1 0 1 0 0 0

日志查询



1 日志查询条件

2 日志查询结果

日志查询条件

1 **磁盘信息** 可选择磁盘型号或者序列号进行查询

2 **擦除功能** 可选择擦除类型或者完成次数进行查询

3 **日期** 可选择擦除操作的起始日期或者结束日期进行查询

日志查询结果

查询条件：磁盘型号-CETC-30 S,开始使用日期至今.

磁盘类型	磁盘序列号	分区号	擦除次数	已完成擦除次数	时间
CETC-30 S	sw_yzyj_10_188	0	1	0	2011-05-22 21:12:12
CETC-30 S	sw_yzyj_10_188	0	1	0	2011-05-22 21:12:37
CETC-30 S	sw_yzyj_10_188	0	1	0	2011-05-23 14:19:46
CETC-30 S	sw_yzyj_10_188	0	1	0	2011-05-23 14:19:46
CETC-30 S	sw_yzyj_10_588	0	1	0	2011-05-23 14:20:00
CETC-30 S	sw_yzyj_10_488	0	1	0	2011-05-23 14:23:49
CETC-30 S	sw_yzyj_10_488	0	1	0	2011-05-23 14:23:49

报表输出

生成查询或审计结果以后，可以将查询或审计结果列表生成报表。在主菜单或工具栏上选择“输出报表”功能，本软件自动将当前的查询或者审计结果生成 Excel 格式的报表。用户可以根据生成的 Excel 格式的报表打印报表，以便存档。

第五章　计算机终端深度检查取证工具

本章内容将帮助您循序渐进地学习使用计算机终端深度检查取证工具(以下简称“取证工具”)。

配置计算机从 USB 设备启动

请参见第四章第一节。

如何启动取证工具

请参见第四章第二节，按类似的步骤启动取证工具。

认识取证工具主界面

1 **快捷菜单栏** 方便用户快速定位到常用功能

2 **功能栏** 按不同功能分类

3 **检查信息栏** 显示检查过程及结果

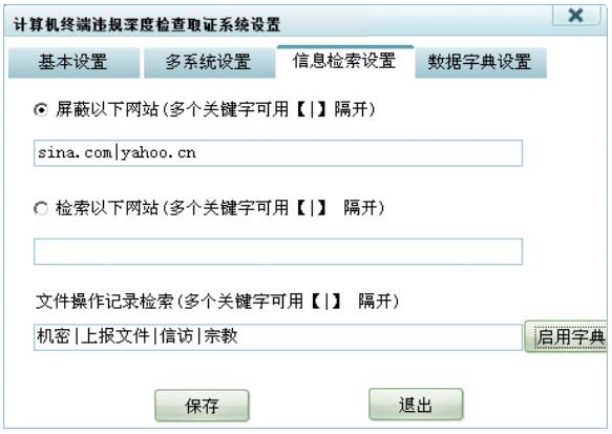
4 **操作日志栏** 历史动

快捷菜单栏

1） 设置：设置检测相关参数；

基本设置：设置检查时间范围、检查数目、检查人、检查单位、受检查人、受检查单位、密级等基本信息

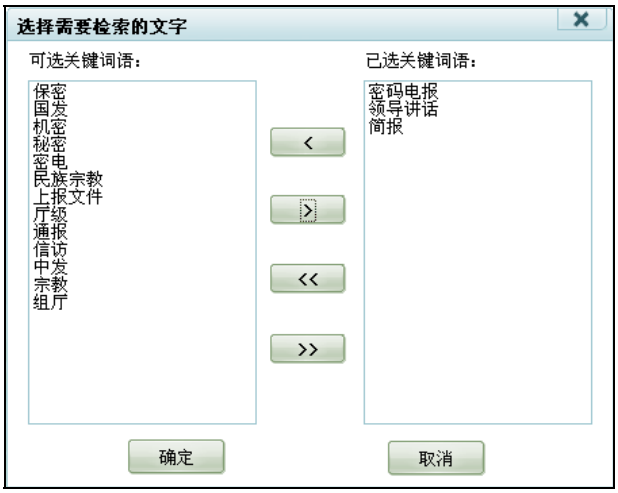
多系统设置：在一台计算机上可能装有多个操作系统，为了保证检测工作的全面性，检查工具支持同时对多个操作系统进行检查，通过复选框，选择你希望检测的操作系统



1 **屏蔽以下网站** 这些网站的访问记录将不会在检查结果中显示

2 **检索以下网站** 这些网站的访问记录将在检查结果中显示

3 **文件操作记录检索** 只显示具有关键字的文件操作记录信息



启用字典：对于一些常用的关键字，保存在字典库，可点击添加

2） 保存：将当前检查项目的检测报告以 doc 文件格式保存到指定目录；

3） 一键保存：将所有检查项目的检测报告以 doc 文件格式保存到指定目录；

4） 一键检测：检查工具自定义了一些重要的常规检查项目，用于快速生成检测报告，对计算机的安全状态做出一个大体的判断；

5） 自定义检查：检查人员可自定义检测项目；

6） 查看日志：查看检查日志，并可导出或打印日志。

7） 快速报表：生成检查结果报表。

8） 返回：返回主菜单。

9） 关机：关闭被检查的计算机；

功能栏

取证工具的功能栏共具有 6 大类 18 小项，每一项都对应了不同的计算机保密检查项目。

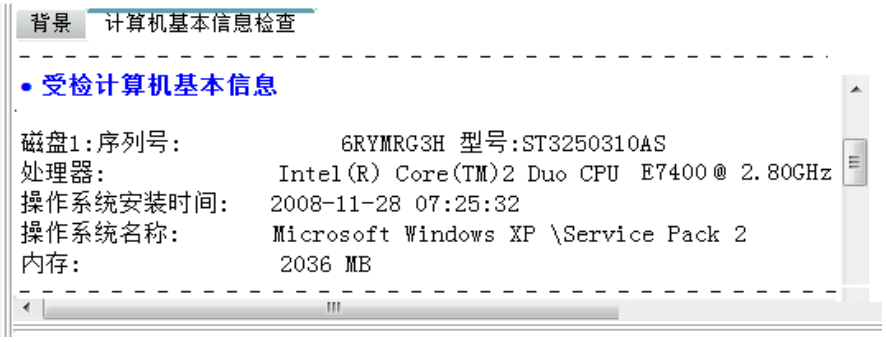
计算机综合检查
计算机基本信息检查
计算机上网信息检查
文件操作信息检查
文件操作记录常规检查
文件操作记录深度检查
文件信息检索
文件信息深度检索
移动介质信息检查
计算机其它信息取证
计算机综合检查
计算机基本信息检查
计算机上网信息检查
文件操作信息检查
移动介质信息检查
移动设备痕迹常规检查
移动设备痕迹深度检查
计算机其它信息取证
计算机综合检查
计算机基本信息检查
计算机上网信息检查
文件操作信息检查
移动介质信息检查
计算机其它信息取证
系统安全检查
安装软件检查
系统日志常规检查
系统日志深度检查
身份鉴别检查

计算机基本信息检查

功能图标： 计算机基本信息检查

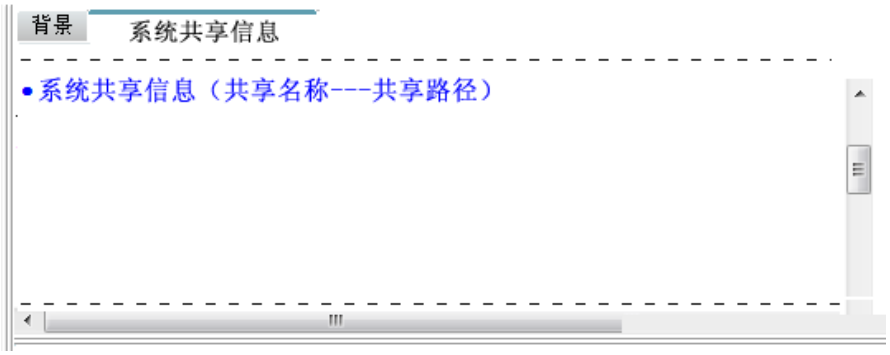
功能：检查计算机的基本信息，如：计算机所安装的操作系统、计算机名、补丁信息、共享信息等软件信息和一些计算机硬件信息。包括下列检测项目：

- 受检计算机基本信息

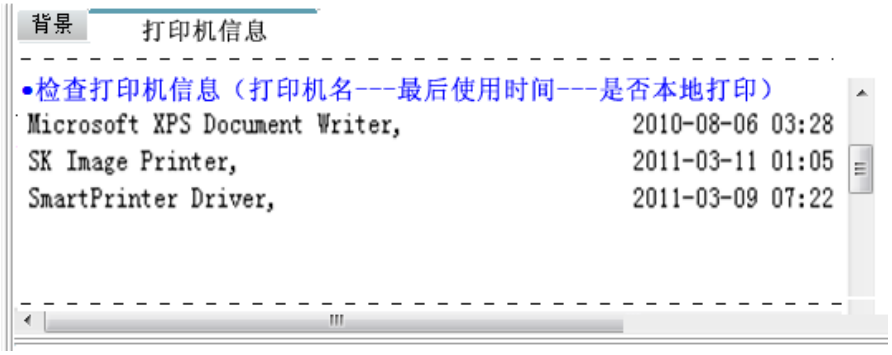


- 补丁安装信息

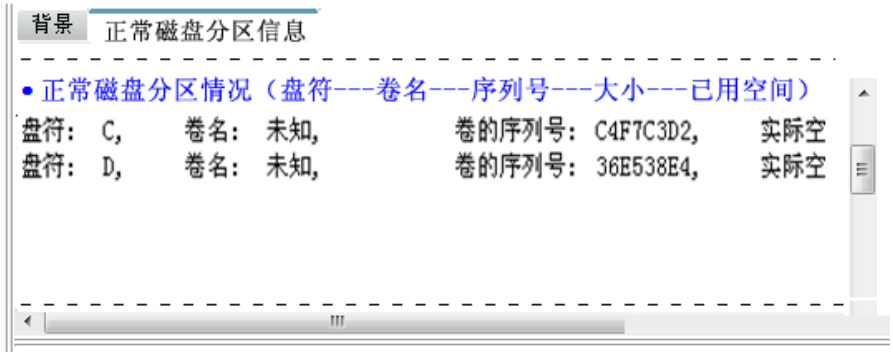
- 检查系统共享



- 打印机信息



- 正常硬盘分区情况



- 检查系统驱动信息

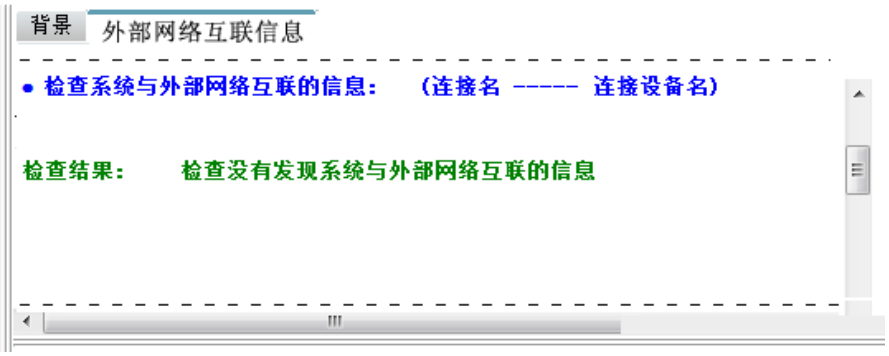
计算机上网信息检查

上网信息常规检查

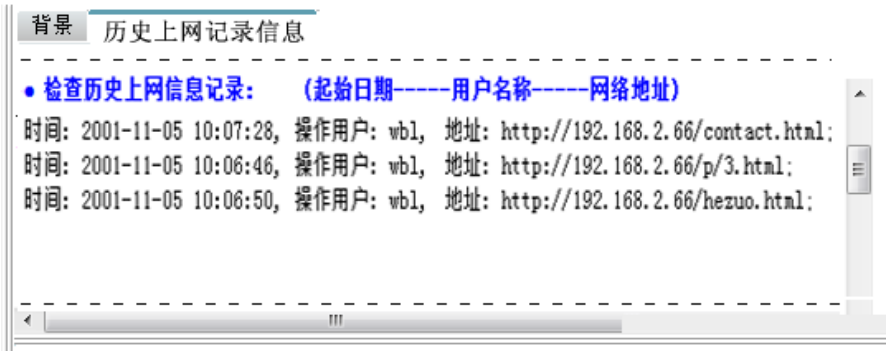
功能图标：上网信息常规检查

功能：检查计算机连接互联网的信息，主要检查计算机与互联网连接设备信息、网页浏览记录以及安装过的网络工具，如：COOKIES 下的记录、TEMP 下的记录、收藏夹下的记录、浏览器下拉列表中的记录。

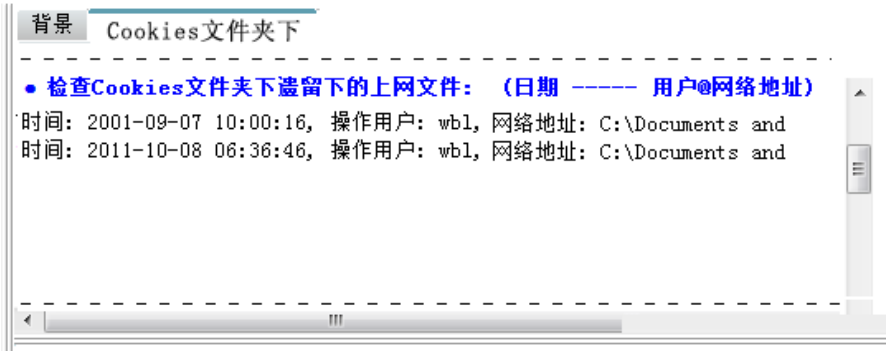
- 检查系统与外部网络互联的信息



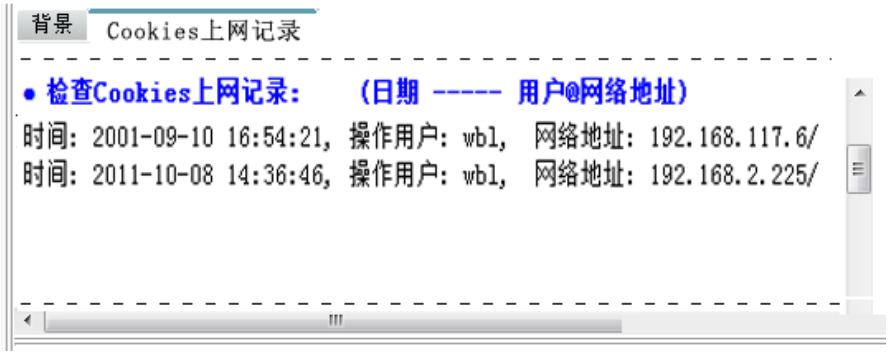
- 检查历史上网信息记录


背景
历史上网记录信息
• 检查历史上网信息记录： （起始日期-----用户名称-----网络地址）
时间: 2001-11-05 10:07:28, 操作用户: wbl, 地址: http://192.168.2.66/contact.html;
时间: 2001-11-05 10:06:46, 操作用户: wbl, 地址: http://192.168.2.66/p/3.html;
时间: 2001-11-05 10:06:50, 操作用户: wbl, 地址: http://192.168.2.66/hezuo.html;

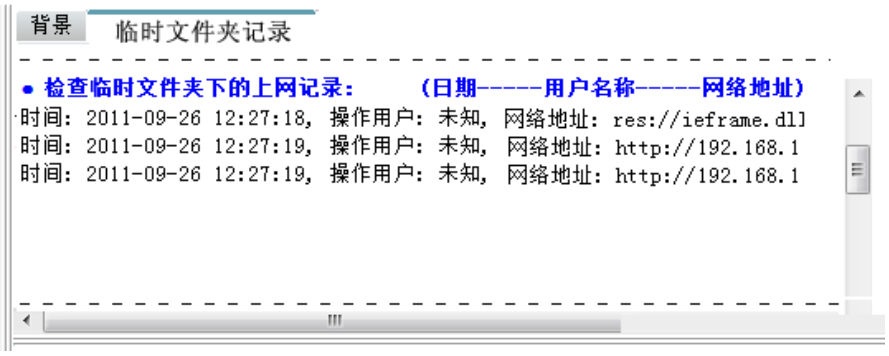
- 检查 Cookies 文件夹下遗留下的上网文件


背景
Cookies文件夹下
• 检查Cookies文件夹下遗留下的上网文件： （日期 ----- 用户@网络地址）
时间: 2001-09-07 10:00:16, 操作用户: wbl, 网络地址: C:\Documents and
时间: 2011-10-08 06:36:46, 操作用户: wbl, 网络地址: C:\Documents and

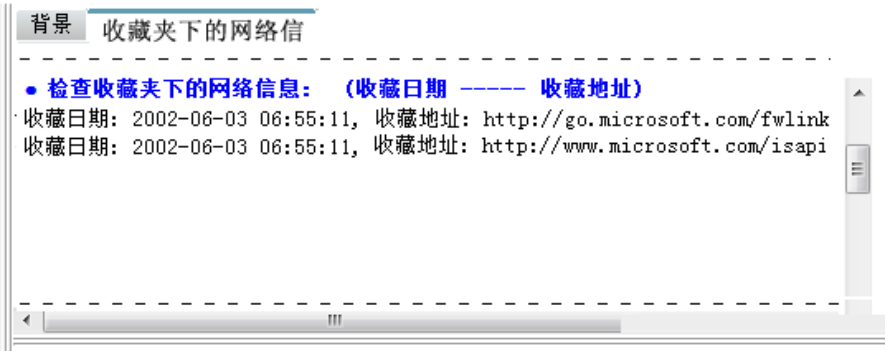
- 检查 Cookies 上网记录


背景
Cookies上网记录
• 检查Cookies上网记录： （日期 ----- 用户@网络地址）
时间: 2001-09-10 16:54:21, 操作用户: wbl, 网络地址: 192.168.117.6/
时间: 2011-10-08 14:36:46, 操作用户: wbl, 网络地址: 192.168.2.225/

- 检查临时文件夹下的上网记录

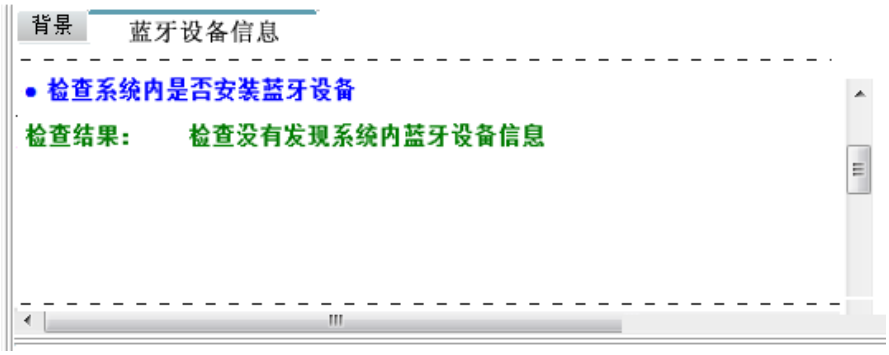


- 检查收藏夹下的网络信息

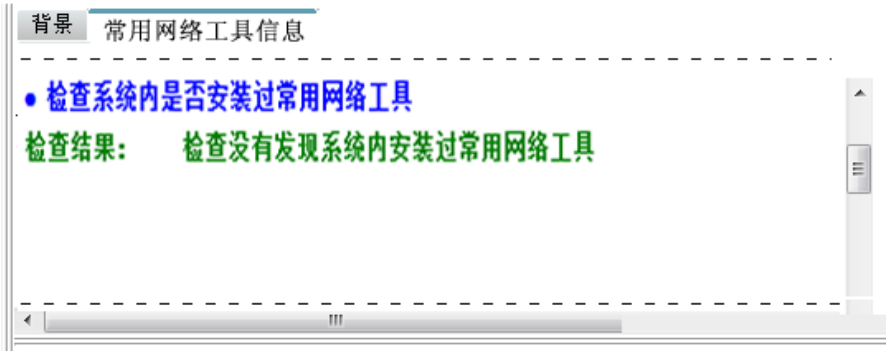


- 检查浏览器地址下拉列表

- 系统是否安装蓝牙设备信息



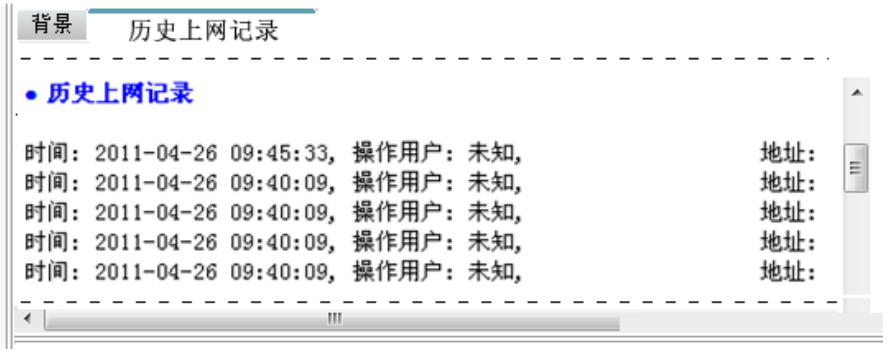
- 系统内是否安装过常用网络工具



上网信息深度检查

功能图标：上网信息深度检查

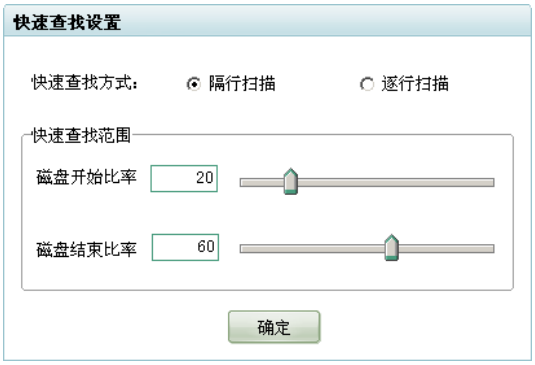
功能：对上网记录的深度检查，能检查出计算机用户已经删除的上网记录。



深度快速检查

功能图标：

功能：快速的对检查方指定的磁盘段进行深度检查，提高效率。



1 **快速查找方式** 隔行扫描强度低，速度快；逐行扫描强度高，速度慢

2 **磁盘开始比率** 扫描磁盘开始位置百分比

3 **磁盘结束比率** 扫描磁盘结束位置百分比

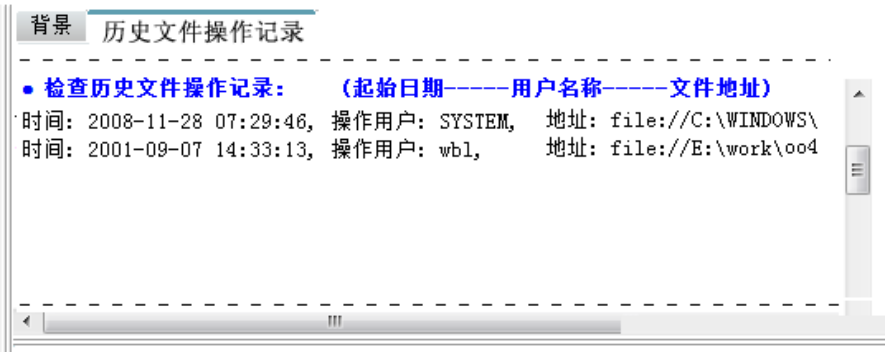
文件操作信息检查

文件操作记录常规检查

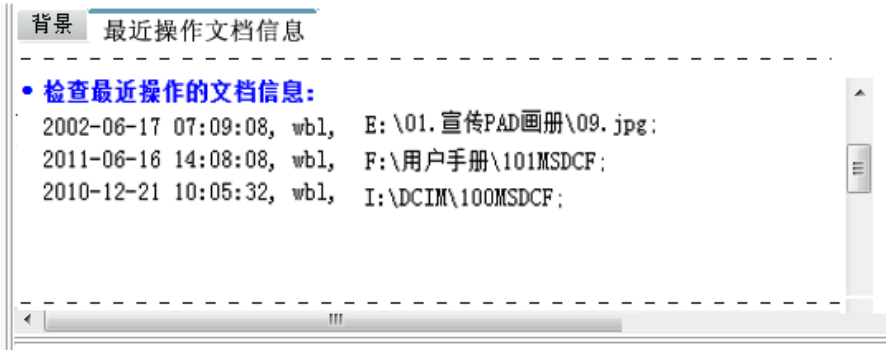
功能图标：

功能：检查出计算机用户对文件的复制、移动、删除操作信息，列出文件操作的时间、用户以及文件路径（包括文件名），包括下列检测项目：

- 检查历史文件操作记录



- 检查最近操作的文档信息

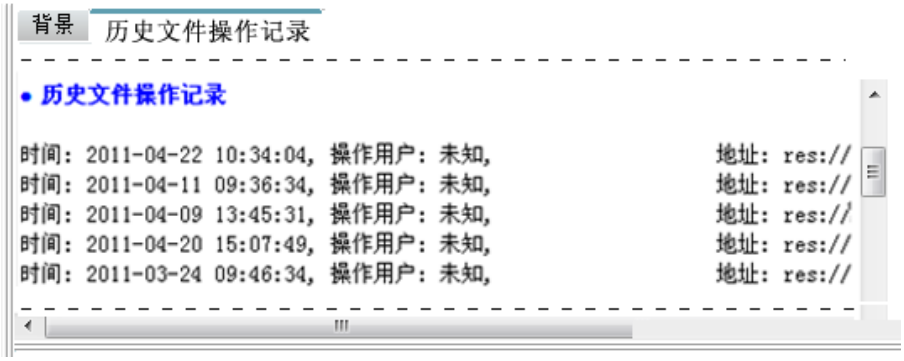


- 检查系统数据库中的文档操作记录信息

文件操作记录深度检查

功能图标：

功能：对文件操作进行深度检查。能检查出许多计算机用户已经清除的文件操作记录。


背景
历史文件操作记录
• 历史文件操作记录
时间: 2011-04-22 10:34:04, 操作用户: 未知, 地址: res://
时间: 2011-04-11 09:36:34, 操作用户: 未知, 地址: res://
时间: 2011-04-09 13:45:31, 操作用户: 未知, 地址: res://
时间: 2011-04-20 15:07:49, 操作用户: 未知, 地址: res://
时间: 2011-03-24 09:46:34, 操作用户: 未知, 地址: res://

文件信息检索

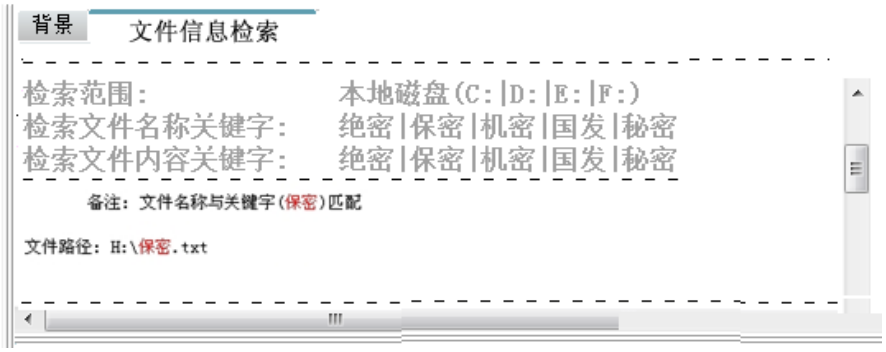
功能图标：文件信息检索

功能：对计算机上存放的文件按照包含的关键字进行检索。如：对计算机上包含有“机密“关键字的文件检索，以便检查一些涉密文件是否存放在计算机上。

1 **可选择检查** 选择检查文件的类型

2 **按文件名搜索** 对在文件名含有关键字的文件进行搜索

3 **按文件内容搜索** 对在文件内容中含有关键字的文件进行搜索



文件信息深度检索

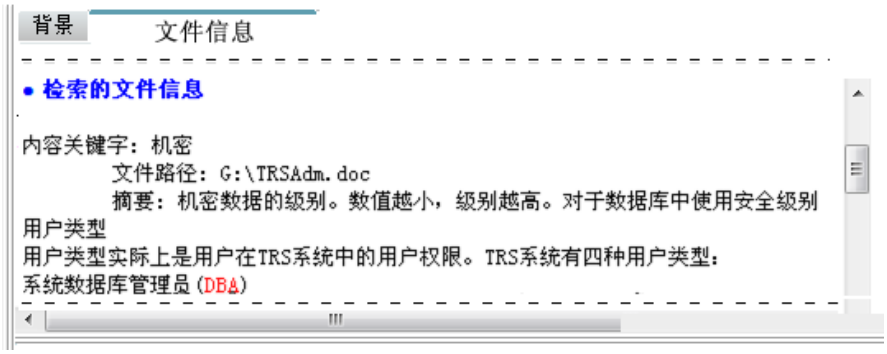
功能图标：文件信息深度检索

功能：对计算机上存放或者存放过的文件进行关键字检索，能检查一些包含关键字的已经删除但可恢复的文件。

1 **可选择检查** 只支持 Microsoft Office 系列文档

2 **按文件名搜索** 对在文件名含有关键字的文件进行搜索

3 **按文件内容搜索** 对在文件内容中含有关键字的文件进行搜索



移动介质信息检查

移动设备痕迹常规检查

功能图标： 移动设备痕迹常规检查

功能：检查在计算机上使用过移动设备的记录，特别是移动存储设备。列出移动设备的名称、序列号、首次在此计算机上使用的时间以及最后一次在此计算机上使用的时间。

移动设备痕迹深度检查

功能图标：

功能：对计算机上使用过移动设备记录进行深度检查，能检查出已经删除的使用记录。

计算机综合检查

一键检查

功能图标：

功能：此功能为一次性检查完所有的常规检查项目。

一键检测常规检查包括以下检测项目：

● 受检计算机基本信息	● 补丁安装信息
● 检查系统共享	● 打印机信息
● 正常硬盘分区情况	● 隐藏磁盘分区情况
● 检查系统驱动信息	● 检查系统与外部网络互联的信息
● 检查历史上网信息记录	● 检查 Cookies 文件夹下的上网文件
● 检查 Cookies 上网记录	● 检查临时文件夹下的上网记录
● 检查收藏夹下的网络信息	● 检查浏览器地址下拉列表
● 检查系统内网络设备信息	● 检查系统内是否安装蓝牙设备
● 检查系统内的蓝牙设备	● 检查历史文件操作记录
● 检查其它文件操作记录	● 检查最近操作的文档信息
● 检查系统数据库中文档信息	● 移动介质痕迹检查记录 1
● 移动介质痕迹检查记录 2	● 进程分析检查
● 检查开放端口信息	● 检查系统服务
● 检查注册表关键位置	● 检查杀毒软件信息
● 检查安装软件	● 系统日志分析检查

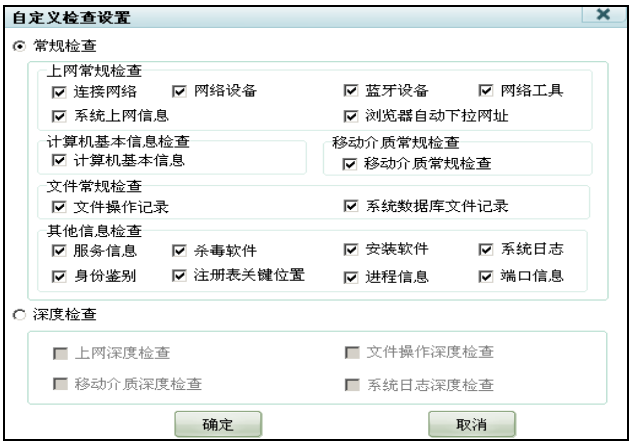
注意：检查分项目的检查内容、检查方式详情请参阅前面章节。

自定义检查

功能图标：

功能：可以对常规检查和深度检查项目进行有选择性的检查。

自定义检测设置框：



1 **常规检查** 对系统中存在的各种信息进行检查

2 **深度检查** 对已删除、重装操作系统、甚至格式化的信息进行磁盘级别的恢复检查

检查综合评估

功能图标：
检查综合评估

功能：对敏感项目进行综合检查评估，包括上网记录及移动介质使用记录，检查速度快。

● 检查系统与外部网络互联的信息	● 检查 Cookies 文件夹下遗留下的上网文件
● 检查临时文件夹下的上网记录	● 检查系统内是否安装过常用网络工具
● 检查历史上网信息记录	● 检查系统内网络设备信息
● 检查收藏夹下的网络信息	● 检查系统内是否安装蓝牙设备
● 检查浏览器地址下拉列表	● 检查 Cookies 文件夹下的上网文件
● 检查 Cookies 上网记录	● 移动介质痕迹检查记录

注意：检查分项目的检查内容、检查方式详情请参阅前面章节。

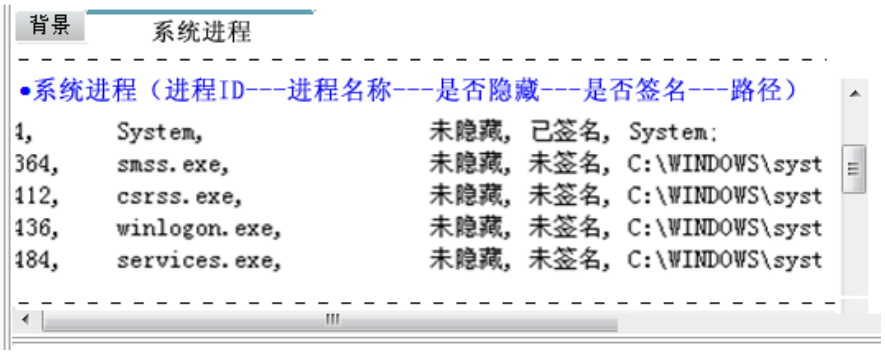
计算机其它信息取证

系统安全检查

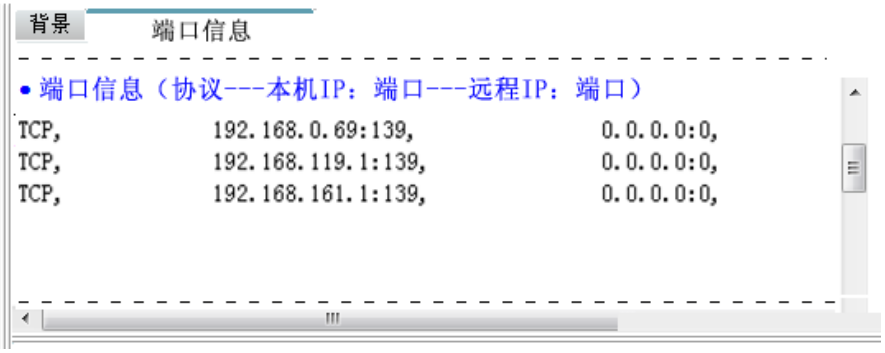
功能图标：
系统安全检查

功能：对系统安全相关的信息进行检查，如：进程、端口、服务、关键注册表以及有无杀毒软件，并列出其各自的基本信息。包含下列检测项目：

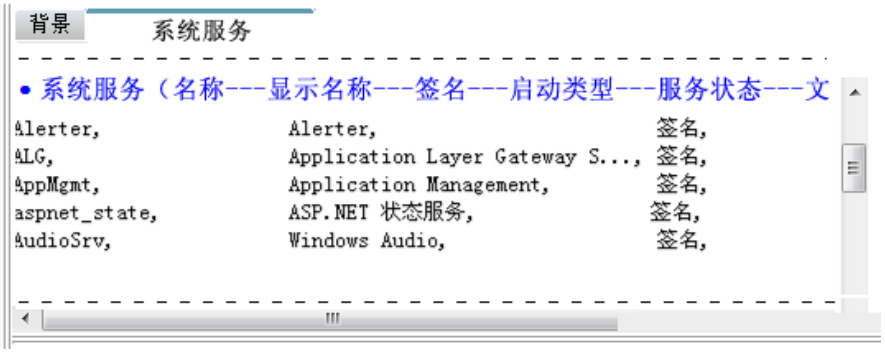
- 进程分析检查；



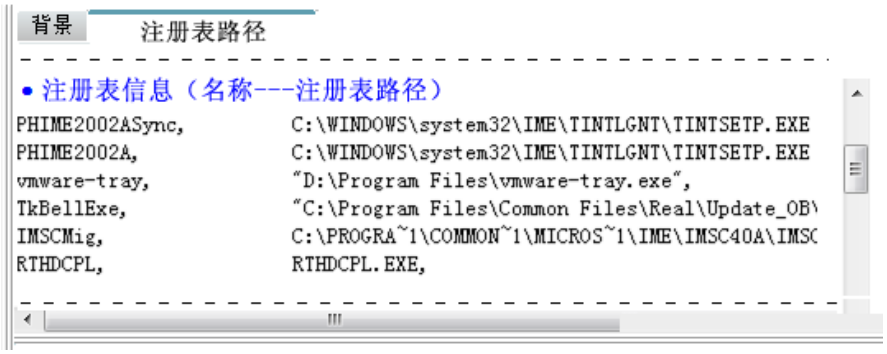
- 检查开放端口信息



- 检查系统服务



- 检查注册表关键位置

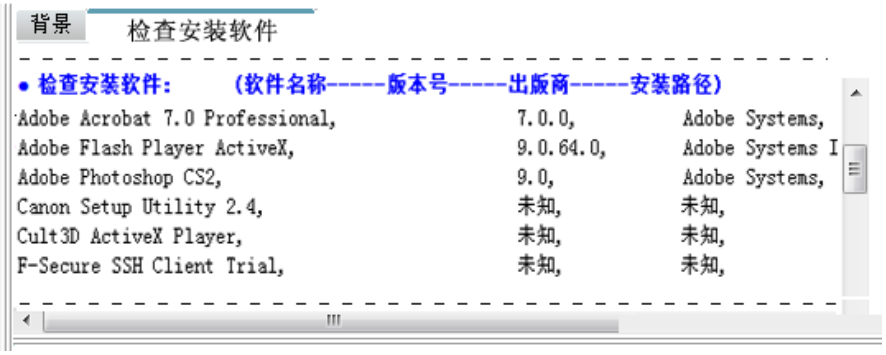


- 检查杀毒软件信息

安装软件检查

功能图标：

功能：检查系统已经安装的软件，并列出其名称、版本号、出版商以及路径。



系统日志常规检查

功能图标：

功能：检查系统记录下的日志信息，并列出其名称、类型、时间等。

系统日志深度检查

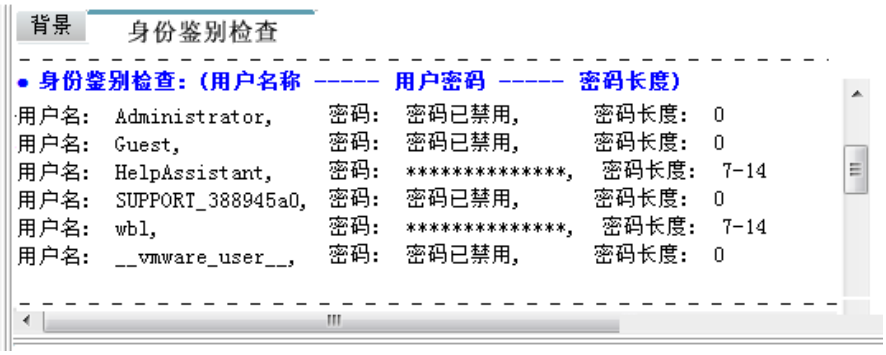
功能图标：

功能：对系统日志进行深度检查，能检查出已经删除的日志记录。

身份鉴别检查

功能图标：

功能：检查操作系统中的用户及密码，会根据位数进行部分隐藏，保护用户指令。


背景
身份鉴别检查
● 身份鉴别检查：（用户名称 ----- 用户密码 ----- 密码长度）
用户名: Administrator, 密码: 密码已禁用, 密码长度: 0
用户名: Guest, 密码: 密码已禁用, 密码长度: 0
用户名: HelpAssistant, 密码: **********, 密码长度: 7-14
用户名: SUPPORT_388945a0, 密码: 密码已禁用, 密码长度: 0
用户名: wbl, 密码: **********, 密码长度: 7-14
用户名: __vmware_user__, 密码: 密码已禁用, 密码长度: 0

第六章　恶意程序攻击行为检测

本章内容将帮助您循序渐进地学习使用恶意程序攻击行为检测工具（以下简称“攻击行为检测工具”）。

配置计算机从 USB 设备启动

请参见第四章第一节。

如何启动攻击行为检测工具

请参见第四章第二节，按类似的步骤启动攻击行为检测工具。

认识行为检测工具主界面

1 **快捷菜单栏** 包括常用的功能键

2 **功能栏** 按不同功能分类

3 **信息栏** 显示检查过程及结果

计算机综合检查

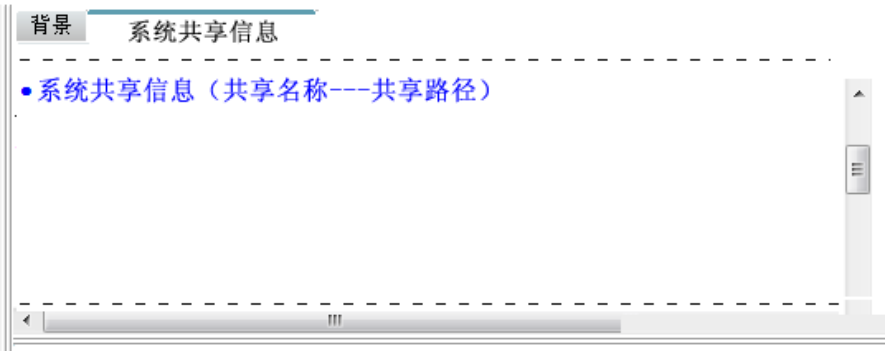
主机安全检查

功能图标：

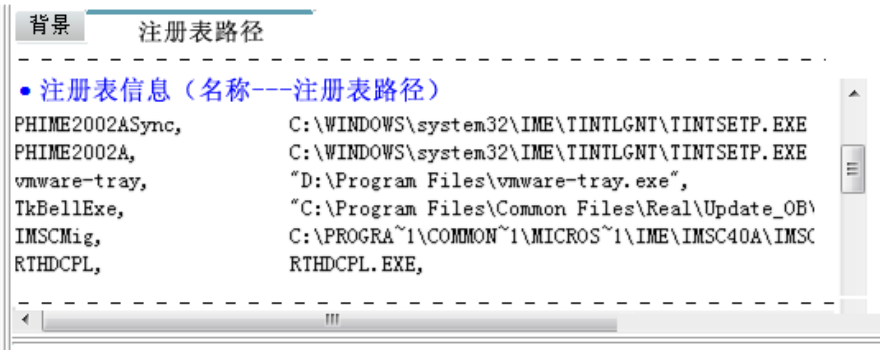
功能：对检查的计算机的安全进行分析，并给出一个可参考的安全指数。

包括下列检测项目:

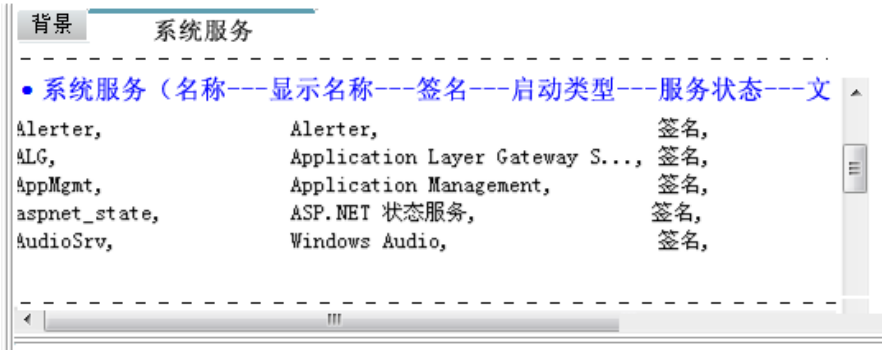
- 检查系统共享



- 系统是否开启远程连接
- 系统是否开启默认磁盘共享
- 系统是否开启默认用户共享
- 检查注册表关键位置



- 检查系统服务



- 检查杀毒软件信息

结论:安全指数

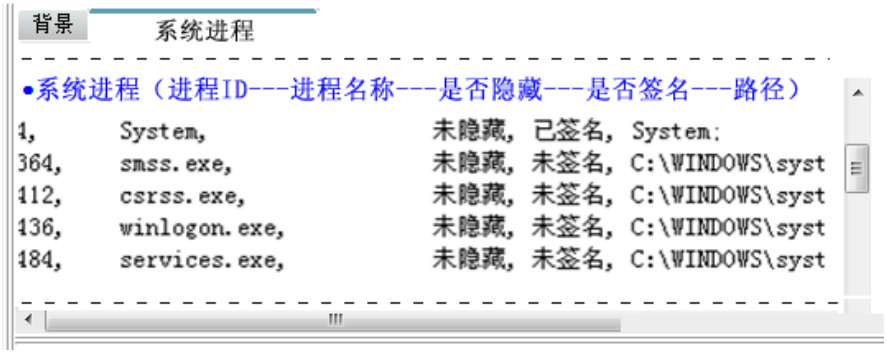
计算机其他信息取证

系统安全检查

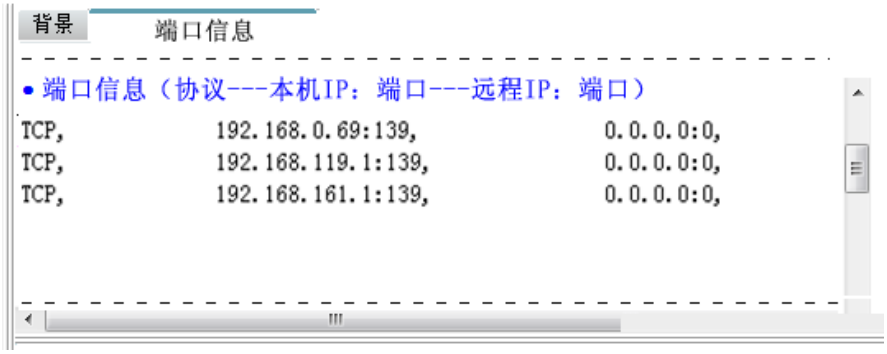
功能图标：

功能：对系统安全相关的信息进行检查，如：进程、端口、服务、关键注册表以及有无杀毒软件，并列出其各自的基本信息。包含下列检测项目：

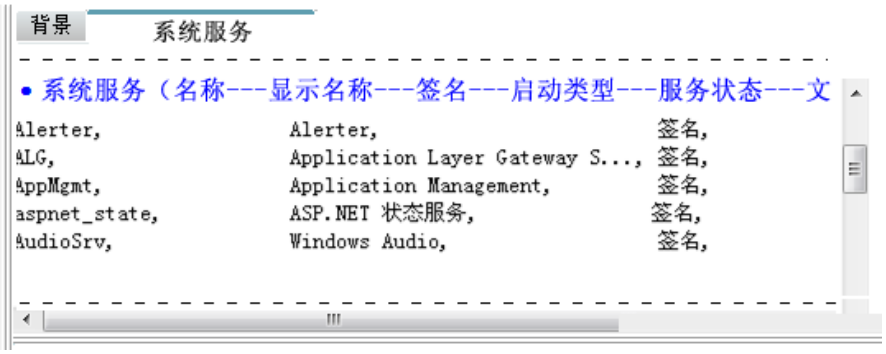
- 进程分析检查；



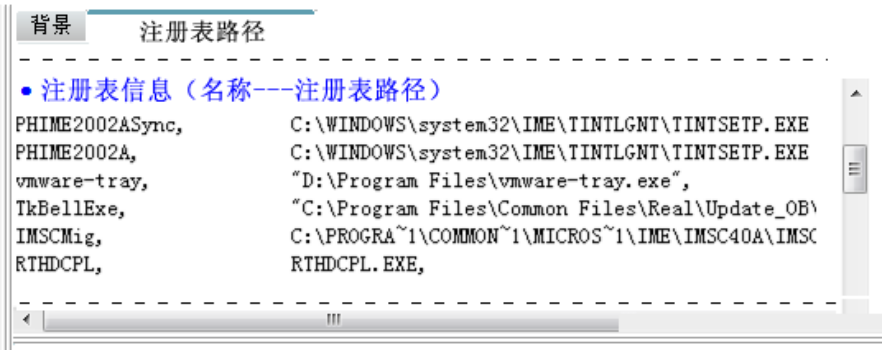
- 检查开放端口信息



- 检查系统服务



- 检查注册表关键位置



- 检查杀毒软件信息

可疑程序扫描

全盘扫描

功能图标： 全盘扫描

功能：对被检查计算机系统内存在可疑程序进行检测，可检查木马、病毒和可疑的恶意程序的位置，并生成检测报告。

点击开始初始化：

运行结果：

快速扫描

功能图标：

功能：只检查计算机的关键位置，检测木马、病毒或可疑的恶意程序的位置，并生成检测报告，作为检查人员对被检查计算机安全等级评估和指导的一个指标。

使用方法同上。

自定义扫描

功能：对被检查计算机的分区选择性进行检查，提高检查效率，可检测木马、病毒和可疑的恶意程序的位置，并生成检测报告。

磁盘分区选择：可选择对磁盘的分区进行检查，缩短检查时间，快速生成检测报告

第七章　常见问题

为什么整盘擦除后磁盘分区没有了?

分区信息是存放在磁盘上特殊区域，由于整盘擦除是对磁盘上的所有数据进行擦除。在进行整盘擦除时，磁盘上的分区信息、文件分配表以及文件内容都被一并擦除掉了。所以经过整盘擦除后磁盘的分区信息没有了，如果要保留磁盘分区信息请选用分区擦除方式。

为什么分区擦除后重新使用该分区需要格式化？

在对分区进行擦除时，为保证不遗留任何痕迹，会将分区上的文件系统信息（BPB- 分区参数块、FAT- 文件分配表、FDT – 文件目录表）一并擦除。所以再重新使用该分区时,需要进行格式化操作重建文件系统。

为什么在启动时临时将平板拔除造成启动失败？

消除工具在启动时，需要从平板电脑 USB 设备中获取重要信息才能正常完成初始化过程。所以在本软件启动时，请不要将平板电脑拔除。

信息消除模式下如何才能退出本软件?

消除工具是建立在独立的 USB 引导系统之上，不依赖于其它任何系统。所以使用完成后需要重启计算机才能恢复到原系统运行。操作方法：在主界面上按“退出擦除”键并选中重启按钮，系统会自动重启 PC，点击重启按钮后请拔除平板与 PC 连接的 USB 串口线，以免 PC 机再次进入擦除模式。

第七章　注意事项

- 本产品擦除磁盘后数据无法恢复，请用户谨慎使用。
- 产品使用后请拔除平板电脑，放置包装盒内妥善保管。
- 作磁盘分区擦除时，请用户务必确认需要擦除的磁盘分区，以免误将其它分区擦除。
- 使用非正版的操作系统软件安装的操作系统本身可能带入网络访问记录以及移动介质使用痕迹，因此在使用本工具消除磁盘信息后，由于安装非正版操作系统引入的各种系统使用痕迹，我方不承担任何责任。
- 在使用本工具完成磁盘信息消除后，用户再次插入涉密介质或访问涉密信息仍然会引入新的使用记录，特别提醒：Windows 操作系统会自动创建目录与文件索引，即使只是插入涉密介质，不访问其中的涉密文件，同样会在 Windows 系统中留下涉密文件的纪录。
- 平板电脑被拔除期间，擦除操作的日志信息不能被保存。
- 日志审计软件输出报表功能需要 Microsoft Office Excel 办公系统支持，如果没有安装就无法使用日志报表打印功能。

第八章　联系我们

中国电子科技集团公司第三十研究所

电　　话：028-85169238

传　　真：028-85169230

邮　　箱：support@30group.com

网　　址：**http://www.30wish.com.cn**

地　　址：四川省成都市高新区创业大道 6 号

感谢您阅读本手册，再次感谢您使用本产品，谢谢！